In the claims:

Following is a complete set of claims as amended with this Response.

1. (Currently Amended) A user terminal capable of communicating with a wireless access network, the user terminal comprising:

a receiver to receive an certificate from an access point of the wireless access network;

a memory to store an identity certificate signed by a certificate authority to be used by the ~~by an~~ access point of the wireless access network to authenticate the user terminal, the identity certificate being based, at least in part, on hardware included in the user terminal; and

a transmitter to send a registration message to the access point after the user is authenticated.

2. (Original) The user terminal of claim 1, wherein the identity certificate includes a serial number of the user terminal.

3. (Original) The user terminal of claim 2, wherein the serial number comprises a Media Access Control (MAC) address of the user terminal.

4. (Original) The user terminal of claim 1, wherein the identity certificate is factory seeded into the memory of the user terminal.

5. (Original) The user terminal of claim 1, wherein the identity certificate authenticates the user terminal to multiple wireless access networks.

6. (Original) A method comprising: authenticating a user terminal of a wireless access network by an access point of the wireless access network using an identity certificate signed by a certificate authority, the identity certificate being bound to user terminal hardware.

7. (Original) The method of claim 6, wherein the identity certificate being bound to user terminal hardware comprises the identity certificate including a serial number of the user terminal.

8. (Original) The method of claim 7, wherein the serial number comprises a Media Access Control (MAC) address of the user terminal.

9. (Original) The method of claim 6, further comprising authenticating the user by an access point of a second wireless access network using the identity certificate.

10. (Original) The method of claim 6, wherein the identity certificate is factory seeded into the user terminal.

11. (Currently Amended) An access point of a wireless access network, the access point comprising:

a receiver to receive an authenticator message from a user terminal capable of communicating with the wireless access network that is requesting access, the authenticator message including an identity certificate of the user terminal signed by a certificate authority, the identity certificate being bound to user terminal hardware and to receive a registration message after receiving the authenticator message; ~~and~~

a processor coupled to the receiver to authenticate the user terminal using the identity certificate; and

a transmitter to send session certificates to the user terminal in response to the registration request.

12. (Original) The access point of claim 11, wherein the identity certificate being bound to user terminal hardware comprises the identity certificate including a serial number of the user terminal.

13. (Original) The access point of claim 12, wherein the serial number comprises a Media Access Control (MAC) address of the user terminal.

14. (Original) The access point of claim 11, wherein the identity certificate is factory seeded into the user terminal.

15. (Currently Amended) A digital certificate to be seeded into a user terminal capable of communicating with a wireless access network, the certificate comprising:

a serial number of the user terminal; an identification of a certificate authority that signs the certificate; and

a signature of the identified certificate authority;

wherein the certificate is scrambled with an authenticator string generated by an access point.

16. (Original) The certificate of claim 15, wherein the serial number comprises a Media Access Control (MAC) address of the user terminal.

17. (Original) The certificate of claim 15, wherein the certificate authenticates the user terminal to multiple wireless access networks.

18. (Currently Amended) A machine-readable medium having stored thereon data representing instructions that, when executed by a processor of an access point of a wireless access network, cause the processor to perform operations comprising:

authenticating a user terminal of a wireless access network using an identity certificate signed by a certificate authority, the identity certificate being bound to user terminal hardware and scrambled with an authenticator string generated by an access point.

19. (Original) The machine-readable medium of claim 18, wherein the identity certificate being bound to user terminal hardware comprises the identity certificate including a serial number of the user terminal.

20. (Original) The machine-readable medium of claim 19, wherein the serial number comprises a Media Access Control (MAC) address of the user terminal.

21. (Original) The machine-readable medium of claim 18, wherein the instructions further cause the processor to authenticate the user by an access point of a second wireless access network using the identity certificate.

22. (Original) The machine-readable medium of claim 18, wherein the identity certificate is factory seeded into the user terminal.